Chin. Ann. Math. Ser. B
41(3), 2020, 361–370
DOI: 10.1007/s11401-020-0203-z

Chinese Annals of Mathematics, Series B

Kloosterman Sums and a Problem of D. H. Lehmer*

Ping XI[1] Yuan YI[1]

(*Dedicated to Professor Wenpeng Zhang on the occasion of his sixtieth birthday*)

Abstract A classical problem of D. H. Lehmer suggests the study of distributions of elements of $\mathbf{Z}/p\mathbf{Z}$ of opposite parity to the multiplicative inverse mod p. Zhang initiated this problem and found an asymptotic evaluation of the number of such elements. In this paper, an asymptotic formula for the fourth moment of the error term of Zhang is proved, from which one may see that Zhang's error term is optimal up to the logarithm factor. The method also applies to the case of arbitrary positive integral moments.

Keywords D. H. Lehmer problem, Kloosterman sum, Moment
2000 MR Subject Classification 11N69, 11L05

1 Introduction

Let q be an odd positive integer and $(c, q) = 1$. We are interested in the set

$$\mathcal{L}_q(c) = \{(x, y) \in [1, q]^2 : xy \equiv c (\operatorname{mod} q), 2 \nmid x + y\}.$$

The original problem of D. H. Lehmer is concerned with the non-trivial information of $\mathcal{L}_q(1)$ (see [3, Section F12] for details). The first attack is due to Zhang [12], who obtained an asymptotic formula for $|\mathcal{L}_q(1)|$ as long as q is a prime power or a product of two distinct primes. Shortly after, he generalized the case to arbitrary odd q and proved in [13] that

$$|\mathcal{L}_q(1)| = \frac{1}{2}\varphi(q) + O(q^{\frac{1}{2}}\tau(q)^2 \log^2 q), \tag{1.1}$$

where τ denotes the divisor function. Various generalizations and extensions can be found in [1, 5–8, 10–11] for instance.

It is natural to ask whether the error term in (1.1) is the best possible in the exponent of q and a good choice is to examine the moment

$$\mathfrak{M}_k(q) := \sideset{}{^*}\sum_{c \bmod q} \Delta_q(c)^k,$$

Manuscript received June 23, 2018. Revised August 30, 2018.

[1] School of Mathematics and Statistics, Xi'an Jiaotong University, Xi'an 710049, China.
E-mail: ping.xi@xjtu.edu.cn yuanyi@xjtu.edu.cn

*This work was supported by the National Natural Science Foundation of China (No. 11601413), the Fundamental Research Funds for the Central Universities (No. 201806078) and the Natural Science Basic Research Plan in Shaanxi Province of China (No. 2017JQ1016).

where

$$\Delta_q(c) := |\mathcal{L}_q(c)| - \frac{1}{2}\varphi(q). \tag{1.2}$$

By virtue of the analytic properties of Dirichlet characters and L-functions, Zhang [14] proved that

$$\mathfrak{M}_2(p) = \frac{3}{4}p^2 + O(p^{1+\varepsilon}) \tag{1.3}$$

for all large prime p and any $\varepsilon > 0$. This was later generalized by Zhang, Xu and Yi [15] to general odd moduli.

In this paper, we focus on higher moments $\mathfrak{M}_k(q)$ with restricting to prime moduli. In particular, we will prove the following asymptotic formula.

Theorem 1.1 *For all large prime p, we have*

$$\mathfrak{M}_4(p) = cp^3 + O(p^{\frac{5}{2}} \log^6 p)$$

with

$$c = \frac{27}{16} - \frac{2336751616}{22153125\pi^8} \sum_{n\geq 1} \frac{\tau(n)^4}{n^4} \approx 1.654.$$

In fact, our method can be generalized to evaluate $\mathfrak{M}_{2k}(p)$ for each integer $k \geq 3$. More precisely, one may prove, there exists some constant c_k, depending only on k, that

$$\mathfrak{M}_{2k}(p) = c_k p^{k+1} + O(p^{k+\frac{1}{2}+\varepsilon}),$$

where the implied constant depends polynomially on k. In the case of odd moments, our argument will also lead to

$$\mathfrak{M}_{2k+1}(p) \ll p^{k+\frac{1}{2}+\varepsilon}$$

for each integer $k \geq 0$, where the implied constant depends polynomially on k. These would require a generalization of Lemma 2.2 (see [2, Proposition 3.2] or [9, Lemma 4] for instance).

By the method of moments, we are then able to prove the probability distribution of $\Delta_p(c)$ as c runs over $(\mathbf{Z}/p\mathbf{Z})^\times$. More precisely, there exists some function $\phi \in \mathcal{C}(\mathbf{R})$, such that for any given $\alpha, \beta \in \mathbf{R}$, we have

$$\lim_{p\to+\infty} \frac{1}{p-1} |\{1 \leq c \leq p-1 : \alpha p^{\frac{1}{2}} \leq \Delta_p(c) \leq \beta p^{\frac{1}{2}}\}| = \int_\alpha^\beta \phi(t)\mathrm{d}t.$$

As another remark, our method also applies to the correlation

$$\sideset{}{^*}\sum_{c \bmod p} \prod_{1\leq i\leq k} \Delta_p(\gamma_i \cdot c),$$

where $\gamma_i \in PGL_2(\mathbf{F}_p)$.

The main tool in this paper is the normalized Kloosterman sum

$$\mathrm{Kl}(x,q)=\frac{1}{\sqrt{q}}\sideset{}{^*}\sum_{a \bmod q}\mathrm{e}\Big(\frac{ax+\overline{a}}{q}\Big).$$

Lemma 2.1 below relates $\Delta_p(c)$ to certain averages of Kloosterman sums. A classical bound of Weil asserts that $|\mathrm{Kl}(x,q)|\leq\tau(q)$, which plays an important role in [13]. To evaluate the moment $\mathfrak{M}_k(p)$, it requires to capture more cancellations among the averages of Kloosterman sums. This starting point is reasonable due to the celebrated work of Katz [4] that the Kloosterman sums $\mathrm{Kl}(x,p)$ become equidistributed in $[-2,2]$ with respected to the Sato-Tate measure, as long as p is large enough. More precisely, we would like to reduce the evaluation of $\mathfrak{M}_k(p)$ to capturing cancellations among Kloosterman sums, and Lemma 2.2 plays a crucial role while picking up the main term for $\mathfrak{M}_4(p)$.

2 Lemmas

The first lemma was already obtained by Zhang [13], which relates the error term $\Delta_p(c)$ to averages of Kloosterman sums in a certain way.

Lemma 2.1 *For $(c,p)=1$, we have*

$$\Delta_p(c)=\frac{p^{\frac12}}{\pi^2}\sum_{1\leq j\leq 2}\sum_{n\leq p^2}\frac{(-1)^j\tau(n,p)}{n}\{\mathrm{Kl}((-1)^jcn,p)-4\mathrm{Kl}((-1)^j\overline{2}cn,p)+4\mathrm{Kl}((-1)^j\overline{4}cn,p)\}$$
$$+O(\log^3 p),$$

where $\tau(n,x):=|\{(a,b)\in[1,x)^2:ab=n\}|$ is a truncated divisor function.

Given $\mathbf{m}=(m_1,m_2,m_3,m_4)\in[1,p-1]^4$, put

$$T(\mathbf{m},p)=\sideset{}{^*}\sum_{x \bmod p}\prod_{1\leq i\leq 4}\mathrm{Kl}(m_ix,p).$$

A crucial part of this paper is to evaluate $T(\mathbf{m},p)$ while $\mathbf{m}$ is in different configurations.

Lemma 2.2 *Keep the above notation.*

(1) *For $m_1\equiv m_2\equiv m_3\equiv m_4(\bmod p)$, we have*

$$T(\mathbf{m},p)=2p+O(p^{\frac12}).$$

(2) *For $m_1\equiv m_2\not\equiv m_3\equiv m_4(\bmod p)$, we have*

$$T(\mathbf{m},p)=p+O(p^{\frac12}).$$

(3) *In the remaining cases up to permutations among m_1,m_2,m_3,m_4, we have*

$$T(\mathbf{m},p)=O(p^{\frac12}).$$

Proof The lemma is a special case of [2, Proposition 3.2] or [9, Lemma 4].

Lemma 2.3 *For any z with $|z| < 1$, we have*

$$\begin{aligned}\sum_{k\geq 0}(k+1)z^k &= \frac{1}{(1-z)^2},\\ \sum_{k\geq 0}(k+1)^2z^k &= \frac{1+z}{(1-z)^3},\\ \sum_{k\geq 0}(k+1)^3z^k &= \frac{1+4z+z^2}{(1-z)^4},\end{aligned}$$

and

$$\sum_{k\geq 0}(k+1)^4z^k = \frac{1+11z+11z^2+z^3}{(1-z)^5}.$$

Proof The above identities can be obtained by differencing

$$\sum_{k\geq 0}z^{k+1} = \frac{z}{1-z}$$

suitably.

Let $\alpha, \beta, \gamma, \delta$ be fixed non-negative integers. Put

$$\begin{aligned}Y(\alpha) &= \sum_{n\geq 1}\frac{\tau(n)\tau(2^\alpha n)}{n^2},\\ Z(\alpha,\beta,\gamma,\delta) &= \sum_{n\geq 1}\frac{\tau(2^\alpha n)\tau(2^\beta n)\tau(2^\gamma n)\tau(2^\delta n)}{n^4}.\end{aligned}$$

Particularly, we write $Z(0) = Z(0,0,0,0)$; i.e.,

$$Z(0) = \sum_{n\geq 1}\frac{\tau(n)^4}{n^4}.$$

Lemma 2.4 *For each given integer $\alpha \geq 0$, we have*

$$Y(\alpha) = \frac{\zeta(2)^4}{\zeta(4)}\Big(\frac{3\alpha}{5}+1\Big).$$

Proof First, we have

$$\begin{aligned}Y(\alpha) &= \sum_{k\geq 0}\frac{1}{4^k}\sum_{\substack{n\geq 1\\ 2\nmid n}}\frac{\tau(2^{k+\alpha}n)\tau(2^k n)}{n^2}\\ &= \sum_{k\geq 0}\frac{(k+\alpha+1)(k+1)}{4^k}\sum_{\substack{n\geq 1\\ 2\nmid n}}\frac{\tau(n)^2}{n^2}.\end{aligned} \tag{2.1}$$

From Lemma 2.3, it follows that

$$\sum_{k\geq 0}\frac{(k+\alpha+1)(k+1)}{4^k} = \sum_{k\geq 0}\frac{(k+1)^2}{4^k} + \alpha\sum_{k\geq 0}\frac{k+1}{4^k} = \frac{16}{9}\Big(\frac{5}{3}+\alpha\Big),$$

and

$$\sum_{\substack{n\geq 1\\ 2\nmid n}}\frac{\tau(n)^2}{n^2}=\prod_{p>2}\sum_{l\geq 0}\frac{\tau(p^l)^2}{p^{2l}}=\prod_{p>2}\sum_{l\geq 0}\frac{(l+1)^2}{p^{2l}}=\prod_{p>2}\frac{1+p^{-2}}{(1-p^{-2})^3}=\frac{27}{80}\frac{\zeta(2)^4}{\zeta(4)},$$

from which and (2.1) the lemma follows.

Lemma 2.5 *For any given non-negative integers $\alpha,\beta,\gamma,\delta$, we have*

$$Z(\alpha,\beta,\gamma,\delta)=\frac{65536}{1794403125}Z(0)Z^*(\alpha,\beta,\gamma,\delta),$$

where

$$\begin{aligned}Z^*(\alpha,\beta,\gamma,\delta)&=37808+25680\alpha+25680\beta+25680\gamma+25680\delta+20400\alpha\beta+20400\alpha\gamma\\&\quad+20400\alpha\delta+20400\beta\gamma+20400\beta\delta+20400\gamma\delta\\&\quad+18000\alpha\beta\gamma+18000\alpha\beta\delta+18000\alpha\gamma\delta+18000\beta\gamma\delta+16875\alpha\beta\gamma\delta.\end{aligned}\tag{2.2}$$

Proof First, we have

$$\begin{aligned}Z(\alpha,\beta,\gamma,\delta)&=\sum_{k\geq 0}\frac{1}{16^k}\sum_{\substack{n\geq 1\\ 2\nmid n}}\frac{\tau(2^{k+\alpha}n)\tau(2^{k+\beta}n)\tau(2^{k+\gamma}n)\tau(2^{k+\delta}n)}{n^4}\\&=\sum_{k\geq 0}\frac{(k+\alpha+1)(k+\beta+1)(k+\gamma+1)(k+\delta+1)}{16^k}\sum_{\substack{n\geq 1\\ 2\nmid n}}\frac{\tau(n)^4}{n^4}.\end{aligned}$$

From Lemma 2.3, it follows that

$$\sum_{k\geq 0}\frac{(k+\alpha+1)(k+\beta+1)(k+\gamma+1)(k+\delta+1)}{16^k}=\frac{16}{253125}Z^*(\alpha,\beta,\gamma,\delta),$$

where $Z^*(\alpha,\beta,\gamma,\delta)$ is given by (2.2). On the other hand,

$$\begin{aligned}\sum_{\substack{n\geq 1\\ 2\nmid n}}\frac{\tau(n)^4}{n^4}&=\prod_{p>2}\sum_{l\geq 0}\frac{\tau(p^l)^4}{p^{4l}}=\prod_{p>2}\sum_{l\geq 0}\frac{(l+1)^4}{p^{4l}}=\prod_{p>2}\frac{1+11p^{-4}+11p^{-16}+p^{-64}}{(1-p^{-4})^5}\\&=\frac{4096}{7089}\prod_{p}\frac{1+11p^{-4}+11p^{-16}+p^{-64}}{(1-p^{-4})^5}=\frac{4096}{7089}\sum_{n\geq 1}\frac{\tau(n)^4}{n^4}.\end{aligned}$$

The lemma then follows by combining all above evaluations.

Lemma 2.6 *Let $\alpha\in\{0,1,2\}$. For sufficiently large q, we have*

$$\sum_{\substack{m,n\leq q^2\\ m\equiv 2^\alpha n(\bmod q)}}\sum\frac{\tau(m,q)\tau(n,q)}{mn}=\frac{Y(\alpha)}{2^\alpha}+O(q^{-1+\varepsilon})$$

for any $\varepsilon>0$.

Proof Put $\sigma = 2^\alpha$. The congruence condition $m \equiv \sigma n (\operatorname{mod} q)$ is equivalent to $m = \sigma n + lq$ for some $l \in \mathbf{Z}$. Note that $m, n \le q^2$, we thus assume $0 \le |l| \ll q$. If $l \ne 0$, we may assume $1 \le l \ll q$ without loss of generality. Therefore,

$$\begin{aligned}\sum_{1\le l\ll q}\ \sum_{\substack{m,n\le q^2\\ m=\sigma n+lq}}\sum \frac{\tau(m,q)\tau(n,q)}{mn} &= \sum_{1\le l\ll q}\ \sum_{n\le q^2}\frac{\tau(\sigma n+lq,q)\tau(n,q)}{n(\sigma n+lq)}\\ &\ll q^\varepsilon \sum_{1\le l\ll q}\ \sum_{n\le q^2}\frac{1}{nlq}\\ &\ll q^{-1+\varepsilon}.\end{aligned}$$

It then follows that

$$\begin{aligned}\sum_{\substack{m,n\le q^2\\ m\equiv\sigma n(\operatorname{mod} q)}}\sum \frac{\tau(m,q)\tau(n,q)}{mn} &= \frac{1}{\sigma}\sum_{n\le q^2}\frac{\tau(\sigma n,q)\tau(n,q)}{n^2}+O(q^{-1+\varepsilon})\\ &= \frac{1}{\sigma}\sum_{n\ge 1}\frac{\tau(\sigma n,q)\tau(n,q)}{n^2}+O(q^{-1+\varepsilon}).\end{aligned}$$

Furthermore, we find

$$\tau(\sigma n,q)=\tau(\sigma n)+O\Big(\sum_{q\le d|\sigma n}1\Big),$$

for which the O-term vanishes unless $\sigma n \ge q$. This observation yields

$$\sum_{\substack{m,n\le q^2\\ m\equiv\sigma n(\operatorname{mod} q)}}\sum \frac{\tau(m,q)\tau(n,q)}{mn} = \frac{1}{\sigma}\sum_{n\ge 1}\frac{\tau(\sigma n)\tau(n)}{n^2}+O(q^{-1+\varepsilon}),$$

from which and Lemma 2.4, the lemma follows immediately.

Lemma 2.7 *Let λ be a fixed positive integer. For sufficiently large q, we have*

$$\sum_{\substack{m,n\le q^2\\ m\equiv-\lambda n\,(\operatorname{mod} q)}}\sum \frac{\tau(m,q)\tau(n,q)}{mn}\ll q^{-1+\varepsilon}$$

for any $\varepsilon > 0$, where the implied constant depends on ε and λ.

Proof The congruence condition $m \equiv -\lambda n (\operatorname{mod} q)$ is equivalent to $m + \lambda n = lq$ for some $l \in \mathbf{Z}$ with $1 \le l \ll q$. We may assume $m \ge \lambda n$ without loss of generality, in which case we find $m \ge \frac{lq}{2}$. Note that

$$\sum_{1\le l\ll q}\ \sum_{\substack{m,n\le q^2\\ m+\lambda n=lq\\ m\ge\lambda n}}\frac{\tau(m,q)\tau(n,q)}{mn}\le \sum_{1\le l\ll q}\ \sum_{\substack{m,n\le q^2\\ m+\lambda n=lq\\ m\ge\lambda n}}\frac{2\tau(m,q)\tau(n,q)}{lqn}\ll q^{-1+\varepsilon}.$$

Then the lemma follows immediately.

3 Proof of Theorem 1.1

3.1 Initial reductions

First, we write

$$\mathfrak{M}_4(p)=\frac{p^2}{\pi^8}\mathfrak{M}_4^*(p)+O(p^{\frac{5}{2}}(\log p)^6), \tag{3.1}$$

where

$$\mathfrak{M}_4^*(p)=\sum_{c \bmod p}^{*}\Big|\sum_{1\leq j\leq 2}\sum_{n\leq p^2}\frac{(-1)^j\tau(n,p)}{n}F(c,j,n;p)\Big|^4$$

and

$$F(c,j,n;p)=\mathrm{Kl}((-1)^j4cn,p)-4\mathrm{Kl}((-1)^j2cn,p)+4\mathrm{Kl}((-1)^jcn,p).$$

Opening the power and switching summations, we get

$$\mathfrak{M}_4^*(p)=\sum_{1\leq j_1,j_2,j_3,j_4\leq 2}\cdots\sum\sum_{n_1,n_2,n_3,n_4\leq p^2}\cdots\sum\frac{(-1)^{j_1+j_2+j_3+j_4}}{n_1n_2n_3n_4}\tau(n_1,p)\tau(n_2,p)\tau(n_3,p)\tau(n_4,p)W(\mathbf{j},\mathbf{n};p),$$

where, for $\mathbf{j}=(j_1,j_2,j_3,j_4),\mathbf{n}=(n_1,n_2,n_3,n_4)$,

$$W(\mathbf{j},\mathbf{n};p)=\sum_{c \bmod p}^{*}\prod_{1\leq i\leq 4}F(c,j_i,n_i;p).$$

Note that

$$\prod_{1\leq i\leq 4}F(c,j_i,n_i;p)=\prod_{1\leq i\leq 4}\{\mathrm{Kl}((-1)^{j_i}4cn_i,p)-4\mathrm{Kl}((-1)^{j_i}2cn_i,p)+4\mathrm{Kl}((-1)^{j_i}cn_i,p)\}.$$

We may split $W(\mathbf{j},\mathbf{n};p)$ as the linear combination of $3^4=81$ terms, each of which is of the shape $T(\mathbf{m},p)$ upon suitable choices for $\mathbf{m}=(m_1,m_2,m_3,m_4)$. In our applications to $W(\mathbf{j},\mathbf{n};p)$, we will take $\mathbf{m}=(m_1,m_2,m_3,m_4)$ to be one of the following tetrads:

$$(\pm c\sigma_1n_1,\pm c\sigma_2n_2,\pm c\sigma_3n_3,\pm c\sigma_3n_4),\quad (\sigma_1,\sigma_2,\sigma_3,\sigma_4)\in\{1,2,4\}^4. \tag{3.2}$$

Given $\mathbf{m}=(m_1,m_2,m_3,m_4),\mathbf{n}=(n_1,n_2,n_3,n_4)\in\mathbf{Z}^4$, we say that $\mathbf{m}$ and $\mathbf{n}$ are equivalent mod p, if at least one of the following conditions holds:

(1) There exists some δ coprime to p, such that $m_i\equiv\delta n_i(\bmod p)$ for each $i=1,2,3,4$;

(2) $(m_1,m_2,m_3,m_4)\equiv(\sigma n_1,\sigma n_2,\sigma n_3,\sigma n_4)(\bmod p)$ for a certain permutation σ.

Due to the symmetry among j_1,j_2,j_3,j_4 and n_1,n_2,n_3,n_4, we find that $T(\mathbf{m},p)$ and $T(\mathbf{n},p)$ give the same contribution to $\mathfrak{M}_4^*(p)$ if $\mathbf{m}$ and $\mathbf{n}$ are equivalent mod p. With this observation, we may characterize $\mathfrak{M}_4^*(p)$ by

$$\begin{aligned}\mathfrak{M}_4^*(p)=513S_1-1040S_2+16S_3+1632S_4-192S_5+96S_6-1280S_7\\+768S_8-768S_9+256S_{10},\end{aligned} \tag{3.3}$$

where

$$S_\ell := \sum_{1\leq j_1,j_2,j_3,j_4\leq 2}\cdots\sum \sum_{n_1,n_2,n_3,n_4\leq p^2}\cdots\sum \frac{(-1)^{j_1+j_2+j_3+j_4}}{n_1n_2n_3n_4}\tau(n_1,p)\tau(n_2,p)\tau(n_3,p)\tau(n_4,p)\mathfrak{S}(\boldsymbol{\alpha}_\ell,\mathbf{j},\mathbf{n};p),$$

where

$$\mathfrak{S}(\boldsymbol{\alpha}_\ell,\mathbf{j},\mathbf{n};p)=\sum_{c \bmod p}{}^{*}\prod_{1\leq i\leq 4}\mathrm{Kl}((-1)^{j_i}\alpha_{i,\ell}n_ic,p)$$

with $\boldsymbol{\alpha}_\ell=(\alpha_{1,\ell},\alpha_{2,\ell},\alpha_{3,\ell},\alpha_{4,\ell})\in\{1,2,4\}^4$ given by

$$\boldsymbol{\alpha}_1=(1,1,1,1),\quad \boldsymbol{\alpha}_2=(2,2,2,1),\quad \boldsymbol{\alpha}_3=(4,4,4,1),\quad \boldsymbol{\alpha}_4=(2,2,1,1),\quad \boldsymbol{\alpha}_5=(4,4,2,1),$$
$$\boldsymbol{\alpha}_6=(4,4,1,1),\quad \boldsymbol{\alpha}_7=(2,1,1,1),\quad \boldsymbol{\alpha}_8=(4,2,2,1),\quad \boldsymbol{\alpha}_9=(4,2,1,1),\quad \boldsymbol{\alpha}_{10}=(4,1,1,1).$$

3.2 Evaluations of $S_\ell, \ell\in\{1,2,3,7,10\}$

Note that

$$\mathfrak{S}(\boldsymbol{\alpha}_1,\mathbf{j},\mathbf{n};p)=T(\mathbf{m},p),\quad \mathbf{m}=((-1)^{j_1}n_1,\ (-1)^{j_2}n_2,\ (-1)^{j_3}n_3,\ (-1)^{j_4}n_4).$$

From Lemma 2.2, it follows that

$$\mathfrak{S}(\boldsymbol{\alpha}_1,\mathbf{j},\mathbf{n};p)=\begin{cases}2p+O(p^{\frac12}), & (-1)^{j_1}n_1\equiv(-1)^{j_2}n_2\equiv(-1)^{j_3}n_3\equiv(-1)^{j_4}n_4 (\bmod p),\\ p+O(p^{\frac12}), & (-1)^{j_1}n_1\equiv(-1)^{j_2}n_2\not\equiv(-1)^{j_3}n_3\equiv(-1)^{j_4}n_4 (\bmod p),\\ p+O(p^{\frac12}), & (-1)^{j_1}n_1\equiv(-1)^{j_2}n_3\not\equiv(-1)^{j_3}n_2\equiv(-1)^{j_4}n_4 (\bmod p),\\ p+O(p^{\frac12}), & (-1)^{j_1}n_1\equiv(-1)^{j_2}n_4\not\equiv(-1)^{j_3}n_2\equiv(-1)^{j_4}n_3 (\bmod p),\\ O(p^{\frac12}), & \text{otherwise,}\end{cases}$$

from which we find

$$\begin{aligned}S_1&=(2p+O(p^{\frac12}))\sum_{\substack{1\leq j_1,j_2,j_3,j_4\leq 2\\ (-1)^{j_1}n_1\equiv(-1)^{j_2}n_2\equiv(-1)^{j_3}n_3\equiv(-1)^{j_4}n_4 (\bmod p)}}\cdots\sum \sum_{n_1,n_2,n_3,n_4\leq p^2}\cdots\sum\prod_{1\leq i\leq 4}\frac{(-1)^{j_i}}{n_i}\tau(n_i,p)\\ &\quad+(3p+O(p^{\frac12}))\sum_{\substack{1\leq j_1,j_2,j_3,j_4\leq 2\\ (-1)^{j_1}n_1\equiv(-1)^{j_2}n_2\not\equiv(-1)^{j_3}n_3\equiv(-1)^{j_4}n_4 (\bmod p)}}\cdots\sum \sum_{n_1,n_2,n_3,n_4\leq p^2}\cdots\sum\prod_{1\leq i\leq 4}\frac{(-1)^{j_i}}{n_i}\tau(n_i,p)\\ &=(-p+O(p^{\frac12}))\sum_{\substack{1\leq j_1,j_2,j_3,j_4\leq 2\\ (-1)^{j_1}n_1\equiv(-1)^{j_2}n_2\equiv(-1)^{j_3}n_3\equiv(-1)^{j_4}n_4 (\bmod p)}}\cdots\sum \sum_{n_1,n_2,n_3,n_4\leq p^2}\cdots\sum\prod_{1\leq i\leq 4}\frac{(-1)^{j_i}}{n_i}\tau(n_i,p)\\ &\quad+(3p+O(p^{\frac12}))\sum_{\substack{1\leq j_1,j_2,j_3,j_4\leq 2\\ (-1)^{j_1}n_1\equiv(-1)^{j_2}n_2,\ (-1)^{j_3}n_3\equiv(-1)^{j_4}n_4 (\bmod p)}}\cdots\sum \sum_{n_1,n_2,n_3,n_4\leq p^2}\cdots\sum\prod_{1\leq i\leq 4}\frac{(-1)^{j_i}}{n_i}\tau(n_i,p).\end{aligned}$$

By Lemmas 2.6–2.7, we further have

$$\begin{aligned}S_1&=(-2p+O(p^{\frac12}))\sum_{n\geq1}\frac{\tau(n)^4}{n^4}+(12p+O(p^{\frac12}))\Big(\sum_{n\geq1}\frac{\tau(n)^2}{n^2}\Big)^2\\ &=(12Y(0)^2-2Z(0,0,0,0))p+O(p^{\frac12}).\end{aligned}$$

Similarly, we have

$$\begin{aligned}
S_2 &= \Big(6Y(0)Y(1) - \frac{1}{4}Z(0,1,1,1)\Big)p + O(p^{\frac{1}{2}}),\\
S_3 &= \Big(3Y(0)Y(2) - \frac{1}{32}Z(0,2,2,2)\Big)p + O(p^{\frac{1}{2}}),\\
S_7 &= (6Y(0)Y(1) - Z(0,0,0,1))p + O(p^{\frac{1}{2}}),\\
S_{10} &= \Big(3Y(0)Y(2) - \frac{1}{2}Z(0,0,0,2)\Big)p + O(p^{\frac{1}{2}}).
\end{aligned}$$

3.3 Evaluations of $S_\ell, \ell \in \{4,5,6,8,9\}$

Note that

$$\mathfrak{S}(\boldsymbol{\alpha}_4, \mathbf{j}, \mathbf{n}; p) = \begin{cases} 2p + O(p^{\frac{1}{2}}), & (-1)^{j_1}2n_1 \equiv (-1)^{j_2}2n_2 \equiv (-1)^{j_3}n_3 \equiv (-1)^{j_4}n_4 (\operatorname{mod} p),\\ p + O(p^{\frac{1}{2}}), & (-1)^{j_1}2n_1 \equiv (-1)^{j_2}2n_2 \not\equiv (-1)^{j_3}n_3 \equiv (-1)^{j_4}n_4 (\operatorname{mod} p),\\ p + O(p^{\frac{1}{2}}), & (-1)^{j_1}2n_1 \equiv (-1)^{j_2}n_3 \not\equiv (-1)^{j_3}2n_2 \equiv (-1)^{j_4}n_4 (\operatorname{mod} p),\\ p + O(p^{\frac{1}{2}}), & (-1)^{j_1}2n_1 \equiv (-1)^{j_2}n_4 \not\equiv (-1)^{j_3}2n_2 \equiv (-1)^{j_4}n_3 (\operatorname{mod} p),\\ O(p^{\frac{1}{2}}), & \text{otherwise.} \end{cases}$$

Hence

$$\begin{aligned}
S_4 = {}& (2p + O(p^{\frac{1}{2}})) \sum_{\substack{1\le j_1,j_2,j_3,j_4\le 2 \\ (-1)^{j_1}2n_1\equiv(-1)^{j_2}2n_2\equiv(-1)^{j_3}n_3\equiv(-1)^{j_4}n_4 (\operatorname{mod} p)}} \!\!\cdots\!\! \sum_{n_1,n_2,n_3,n_4\le p^2} \prod_{1\le i\le 4} \frac{(-1)^{j_i}}{n_i}\tau(n_i,p)\\
&+ (p + O(p^{\frac{1}{2}})) \sum_{\substack{1\le j_1,j_2,j_3,j_4\le 2 \\ (-1)^{j_1}2n_1\equiv(-1)^{j_2}2n_2\not\equiv(-1)^{j_3}n_3\equiv(-1)^{j_4}n_4 (\operatorname{mod} p)}} \!\!\cdots\!\! \sum_{n_1,n_2,n_3,n_4\le p^2} \prod_{1\le i\le 4} \frac{(-1)^{j_i}}{n_i}\tau(n_i,p)\\
&+ (2p + O(p^{\frac{1}{2}})) \sum_{\substack{1\le j_1,j_2,j_3,j_4\le 2 \\ (-1)^{j_1}2n_1\equiv(-1)^{j_2}n_3\not\equiv(-1)^{j_3}2n_2\equiv(-1)^{j_4}n_4 (\operatorname{mod} p)}} \!\!\cdots\!\! \sum_{n_1,n_2,n_3,n_4\le p^2} \prod_{1\le i\le 4} \frac{(-1)^{j_i}}{n_i}\tau(n_i,p)\\
= {}& (-p + O(p^{\frac{1}{2}})) \sum_{\substack{1\le j_1,j_2,j_3,j_4\le 2 \\ (-1)^{j_1}2n_1\equiv(-1)^{j_2}2n_2\equiv(-1)^{j_3}n_3\equiv(-1)^{j_4}n_4 (\operatorname{mod} p)}} \!\!\cdots\!\! \sum_{n_1,n_2,n_3,n_4\le p^2} \prod_{1\le i\le 4} \frac{(-1)^{j_i}}{n_i}\tau(n_i,p)\\
&+ (p + O(p^{\frac{1}{2}})) \sum_{\substack{1\le j_1,j_2,j_3,j_4\le 2 \\ (-1)^{j_1}n_1\equiv(-1)^{j_2}n_2,\ (-1)^{j_3}n_3\equiv(-1)^{j_4}n_4 (\operatorname{mod} p)}} \!\!\cdots\!\! \sum_{n_1,n_2,n_3,n_4\le p^2} \prod_{1\le i\le 4} \frac{(-1)^{j_i}}{n_i}\tau(n_i,p)\\
&+ (2p + O(p^{\frac{1}{2}})) \sum_{\substack{1\le j_1,j_2,j_3,j_4\le 2 \\ (-1)^{j_1}2n_1\equiv(-1)^{j_2}n_3,\ (-1)^{j_3}2n_2\equiv(-1)^{j_4}n_4 (\operatorname{mod} p)}} \!\!\cdots\!\! \sum_{n_1,n_2,n_3,n_4\le p^2} \prod_{1\le i\le 4} \frac{(-1)^{j_i}}{n_i}\tau(n_i,p).
\end{aligned}$$

From Lemmas 2.6–2.7, we may conclude that

$$S_4 = \Big(4Y(0)^2 + 2Y(1)^2 - \frac{1}{2}Z(0,0,1,1)\Big)p + O(p^{\frac{1}{2}}).$$

Similarly, we have

$$\begin{aligned}
S_5 &= \Big(2Y(0)Y(1) + Y(1)Y(2) - \frac{1}{16}Z(0,1,2,2)\Big)p + O(p^{\frac{1}{2}}),\\
S_6 &= \Big(4Y(0)^2 + \frac{1}{2}Y(2)^2 - \frac{1}{8}Z(0,0,2,2)\Big)p + O(p^{\frac{1}{2}}),\\
S_8 &= \Big(2Y(1)^2 + Y(0)Y(2) - \frac{1}{8}Z(0,1,1,2)\Big)p + O(p^{\frac{1}{2}}),\\
S_9 &= \Big((2Y(0)Y(1) + Y(1)Y(2) - \frac{1}{4}Z(0,0,1,2)\Big)p + O(p^{\frac{1}{2}}).
\end{aligned}$$

3.4 Concluding Theorem 1.1

Inserting all above asymptotic evaluations for S_ℓ to (3.3) and in view of Lemmas 2.4–2.5, we arrive at

$$\mathfrak{M}_4^*(p) = \frac{27}{16}\pi^8 - \frac{2336751616}{22153125}Z(0),$$

from which and (3.1) we conclude Theorem 1.1.

Acknowledgements The authors are grateful to Professor Wenpeng Zhang for all kind help and inspirations in the past years. Thanks are also due to the referee for valuable suggestions.

References

[1] Cobeli, C. and Zaharescu, A., Generalization of a problem of Lehmer, *Manuscripta Math.,* **104**, 2001, 301–307.

[2] Fouvry, É., Ganguly, S., Kowalski, E. and Michel, Ph., Gaussian distribution for the divisor function and Hecke eigenvalues in arithmetic progressions, *Comment. Math. Helv.,* **89**, 2014, 979–1014.

[3] Guy, R. K., Unsolved Problems in Number Theory, 2nd ed., Springer-Verlag, New York, 1994.

[4] Katz, N. M., Gauss Sums, Kloosterman Sums, and Monodromy Groups, Annals of Mathematics Studies, **116**, Princeton University Press, Princeton, NJ, 1988.

[5] Liu, H. N. and Zhang, W. P., Hybrid mean value for a generalization of a problem of D. H. Lehmer, *Acta Arith.,* **130**, 2007, 1–17.

[6] Lu, Y. M. and Yi, Y., On the generalization of the D. H. Lehmer problem, *Acta Math. Sin.* (*Engl. Ser.*)*,* **25**, 2009, 1269–1274.

[7] Ruzsa, I. Z. and Schinzel, A., An application of Kloosterman sums, *Compositio Math.,* **96**, 1995, 323–330.

[8] Shparlinski, I. E., On a generalisation of a Lehmer problem, *Math. Z.,* **263**, 2009, 619–631.

[9] Xi, P., Gaussian distributions of Kloosterman sums: Vertical and horizontal, *Ramanujan J.,* **43**, 2017, 493–511.

[10] Xu, Z. F. and Zhang, T. P., High-dimensional D. H. Lehmer problem over short intervals, *Acta Math. Sin.* (*Engl. Ser.*)*,* **30**, 2014, 213–228.

[11] Yi, Y. and Zhang, W. P., On the generalization of a problem of D. H. Lehmer, *Kyushu J. Math.,* **56**, 2002, 235–241.

[12] Zhang, W. P., On a problem of D. H. Lehmer and its generalization, *Compositio Math.,* **86**, 1993, 307–316.

[13] Zhang, W. P., On a problem of D. H. Lehmer and its generalization. II, *Compositio Math.,* **91**, 1994, 47–56.

[14] Zhang, W. P., A problem of D. H. Lehmer and its mean square value formula, *Japan. J. Math.* (*N.S.*)*,* **29**, 2003, 109–116.

[15] Zhang, W. P., Xu, Z. B. and Yi, Y., A problem of D. H. Lehmer and its mean square value formula, *J. Number Theory,* **103**, 2003, 197–213.